RSAC 2025 Conference

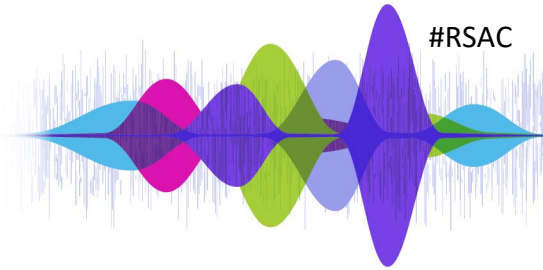
Many Voices.
One Community.

SESSION ID: PART1-W02

Hybrid Mesh Firewall: Overcoming Limitations of Traditional Firewalling

April 30, 2025

Rick Miles, Cisco Security
Randy Pope, Cisco Security

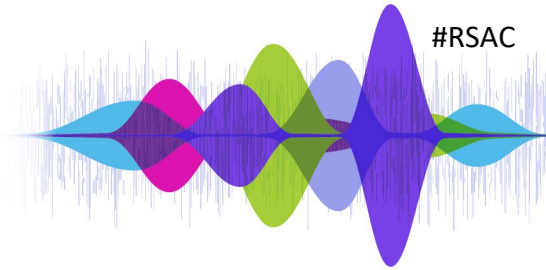


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

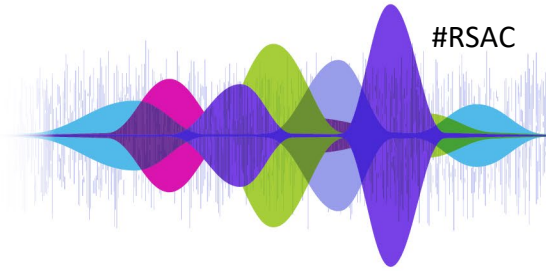
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



Key Takeaways

- **Educate**
  - Describe the importance of the shift towards hybrid mesh firewall solutions, and why now
- **Learn**
  - Understand why a security mesh is critical to protect the AI-ready data center and the critical capabilities needed for successful implementation
- **Apply**
  - Take core capabilities learned within presentation and determine how this approach can benefit your organization today
  - Implement a unified segmentation strategy that aligns with your objectives (regulatory compliance, internal mandates, customer requirements)
  - Skillfully deal with encrypted traffic at scale
  - Assess your risk of your current AI applications and models; apply guard rails for safe and secure use of AI

Securing the enterprise is increasingly challenging



Highly distributed, fine-grained apps

- Spanning data center, cloud
- Containers
- 1000s of microservices

Nothing can be trusted

- Distributed perimeter necessary but no longer sufficient
- Need security in every flow to stop lateral movement

More vulnerabilities, exploited faster

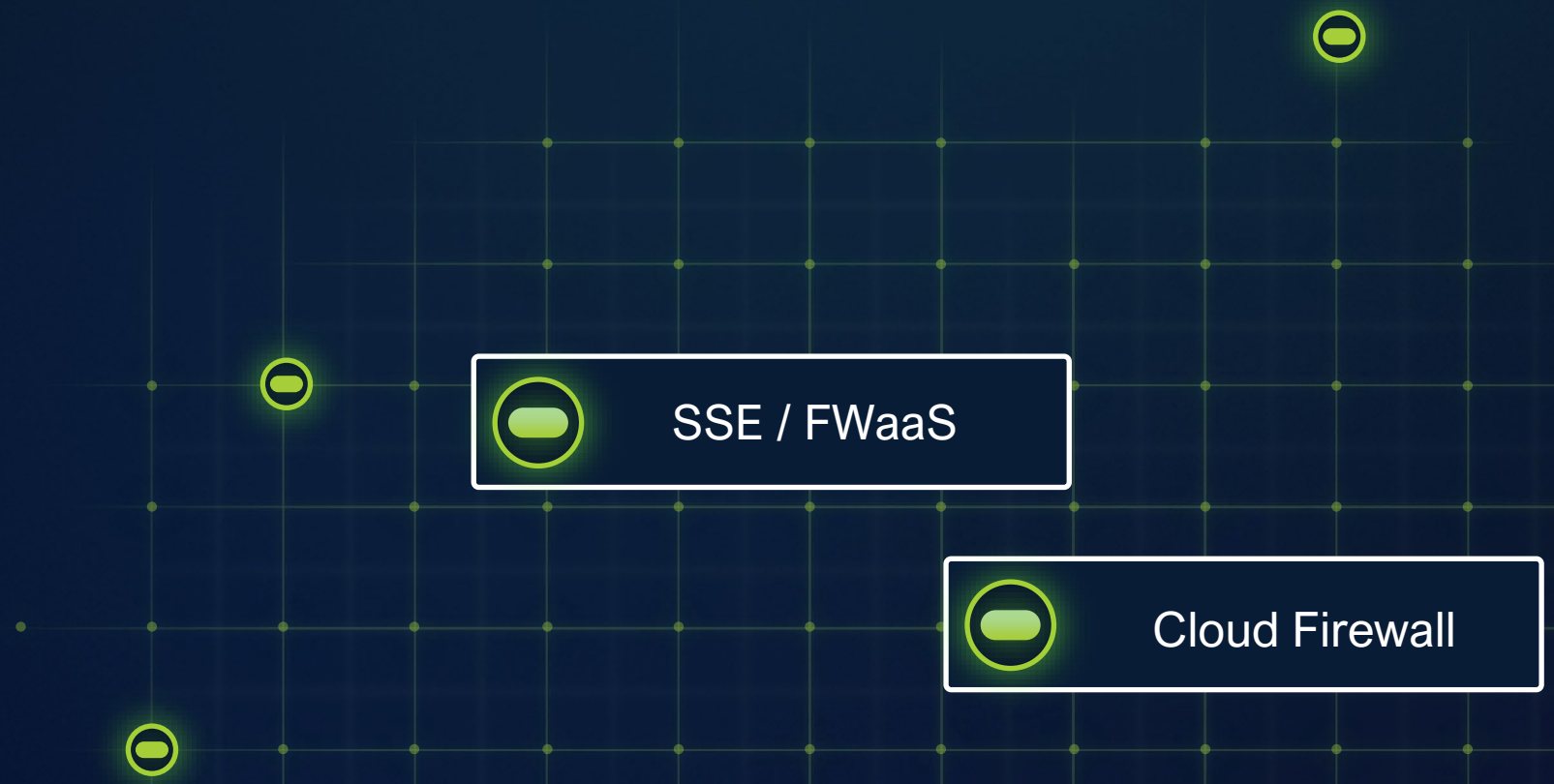
- Weeks to hours to minutes
- Patching can't keep up
- New AI model risks

AI increasing attack surface and attack sophistication

Requirements for successful hybrid mesh firewalling

Next-Generation Firewall

High-performance | Encrypted traffic at scale | Cloud-native

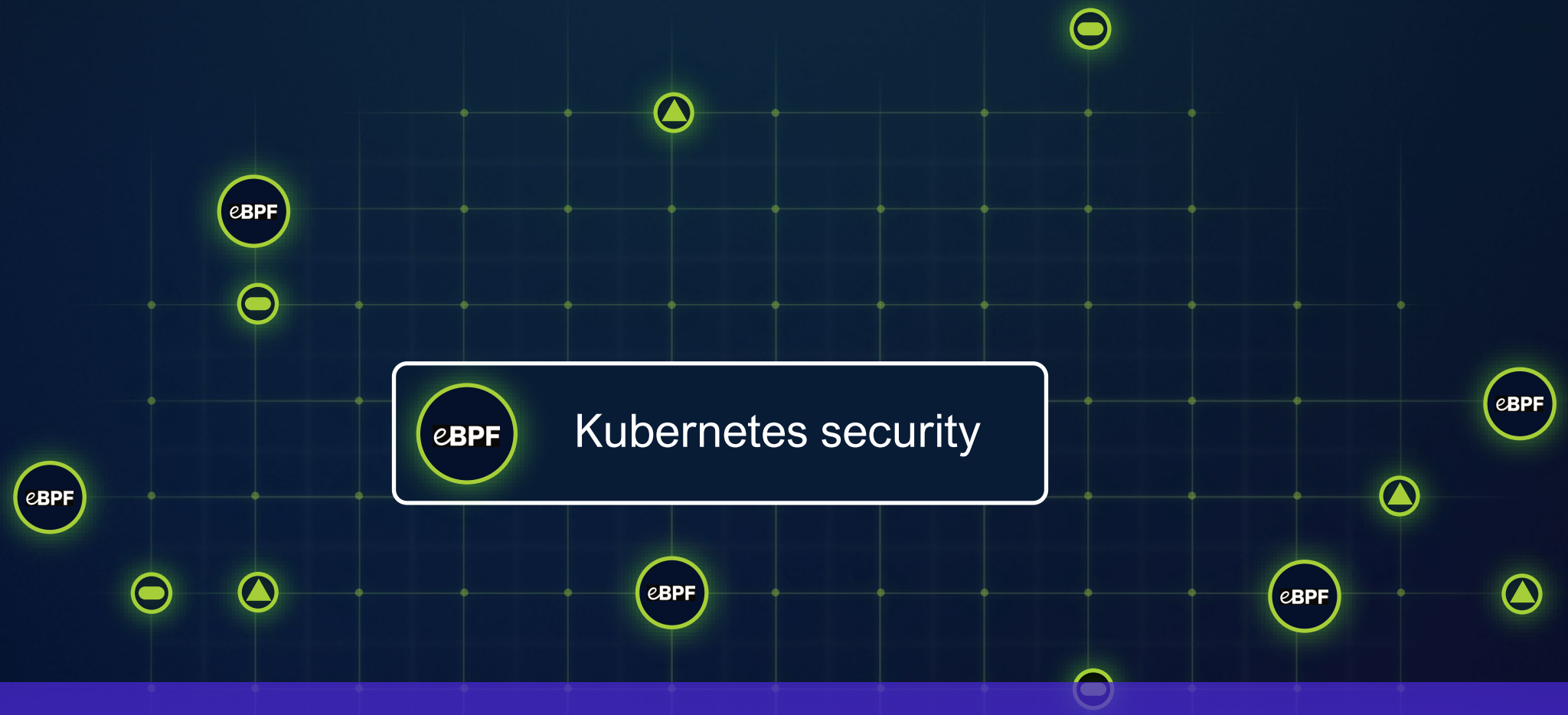


Security Service Edge with FWaaS

Cloud Firewall

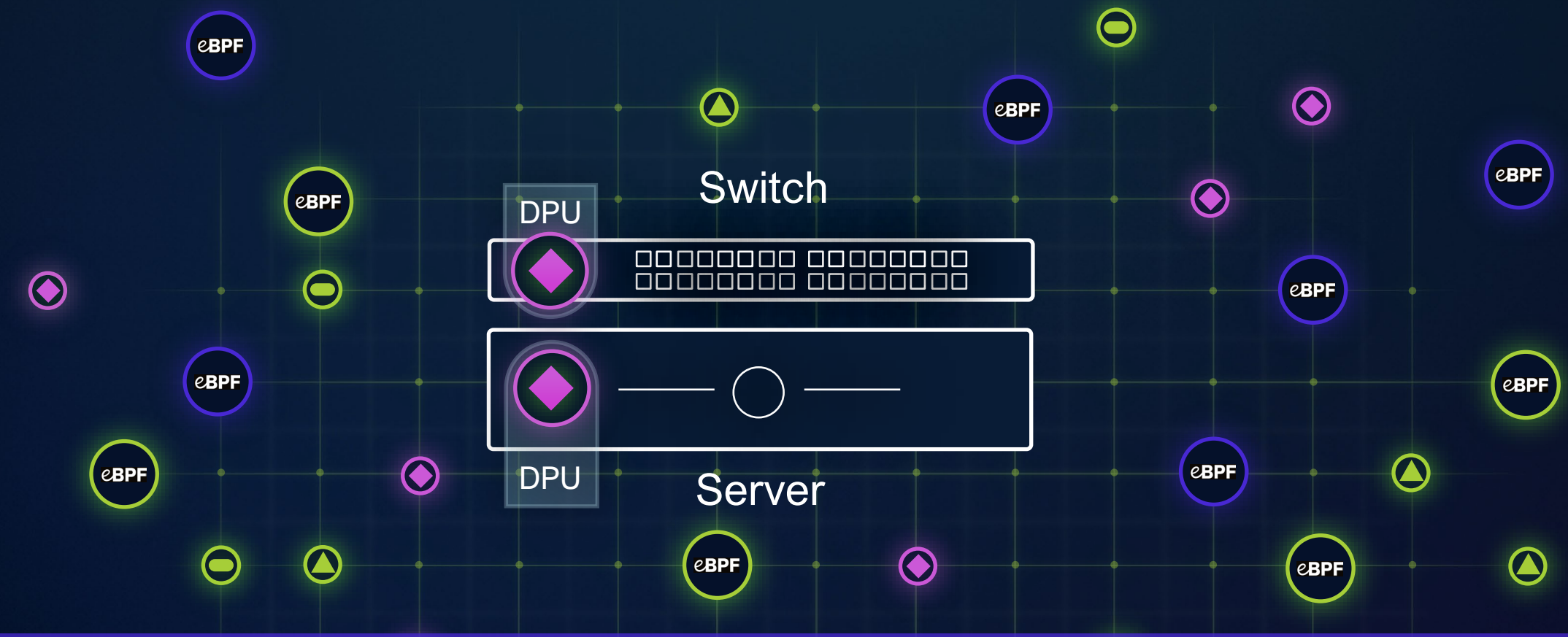
Traditional microsegmentation

Highly scalable | Broad platform support | SaaS option



A network fabric for modern apps

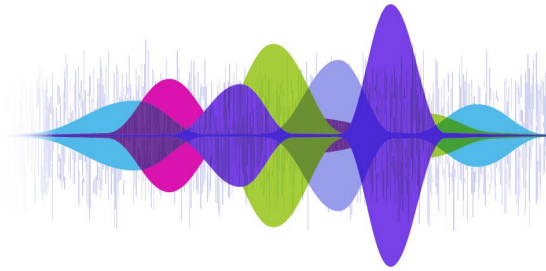
AI-based segmentation | Distributed exploit protection



Tightly integrated with the network

via Smart Switches

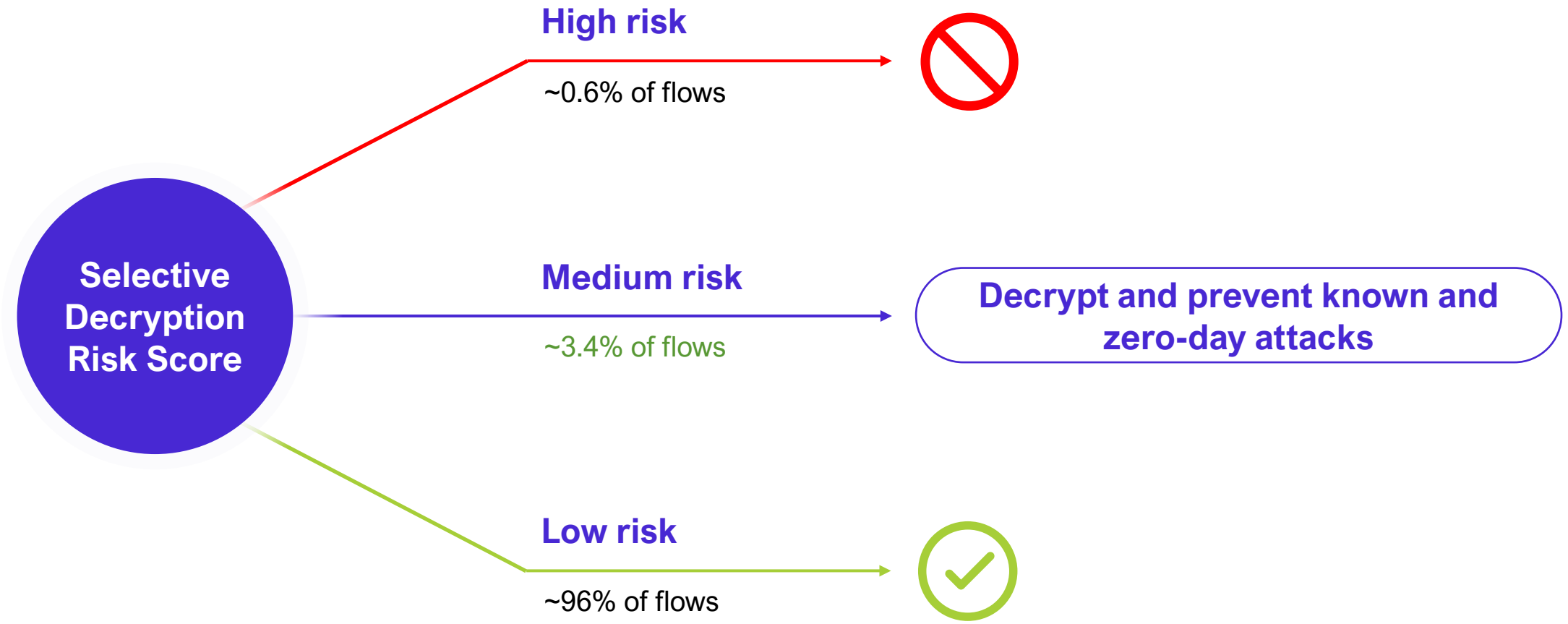
Policy rationalization across firewall vendors



On Prem
Webservers
Finance-frontend
Middleware
Finance-processing
database
Finance-db
http://
AWS
App VPC
K8-apps
Finance-app chatbot
K8
Node
Pod = Front End (replica)
Pod = Database (replica)
Namespace = Finance-App

Security without sacrificing performance

Risk-based intelligent decryption



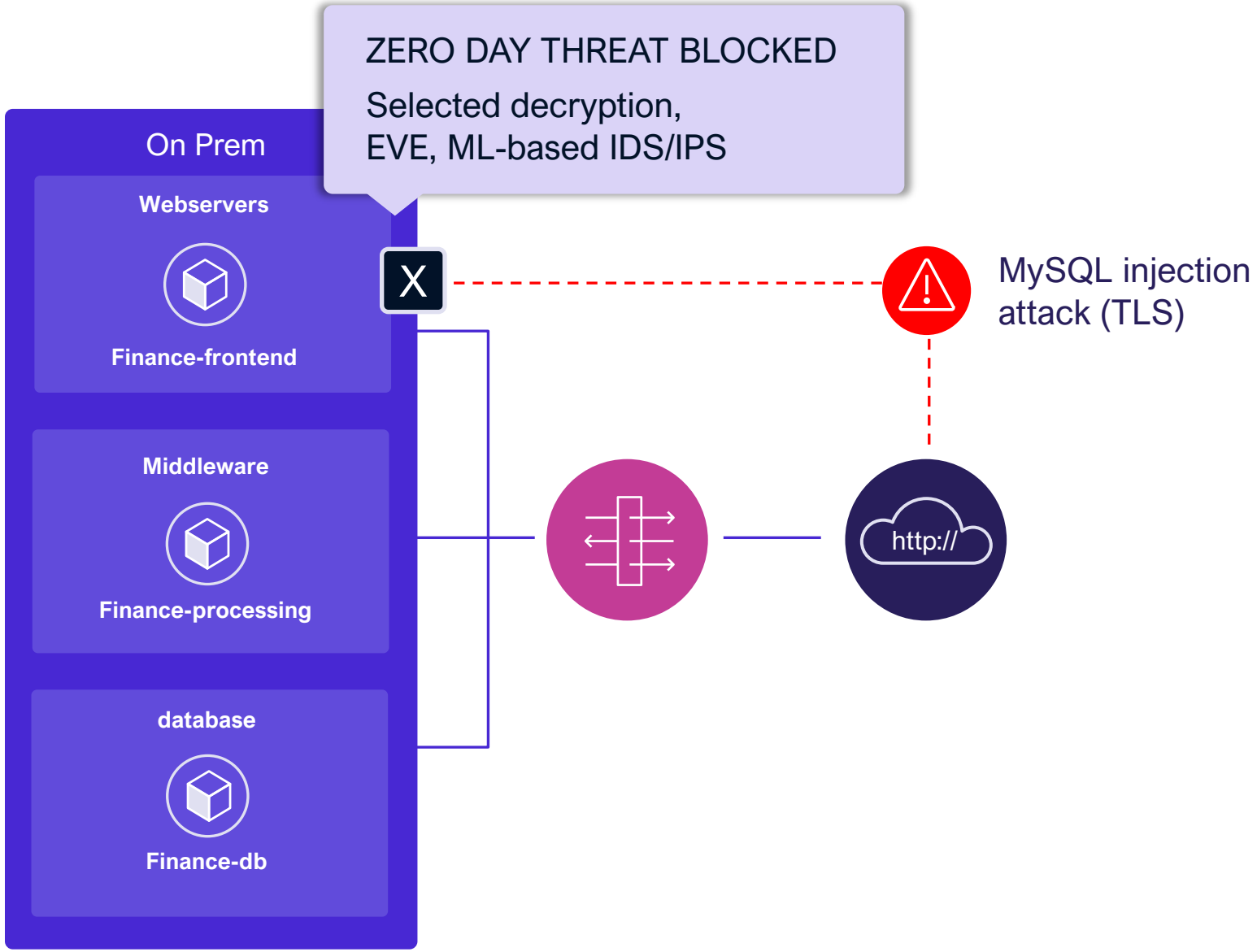
Prevent malicious TLS

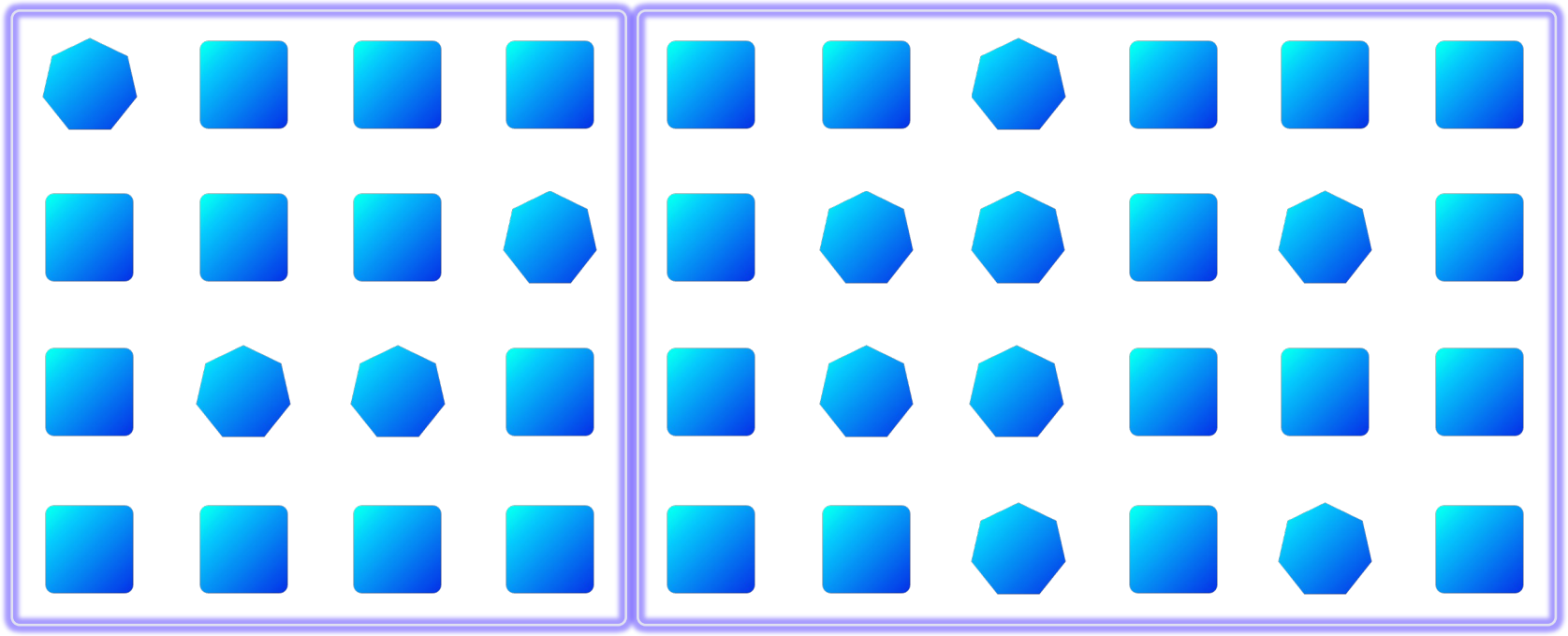
Secure application

Identify vulnerabilities

Deploy / secure cloud environments

Prevent exploits




Dev
Prod

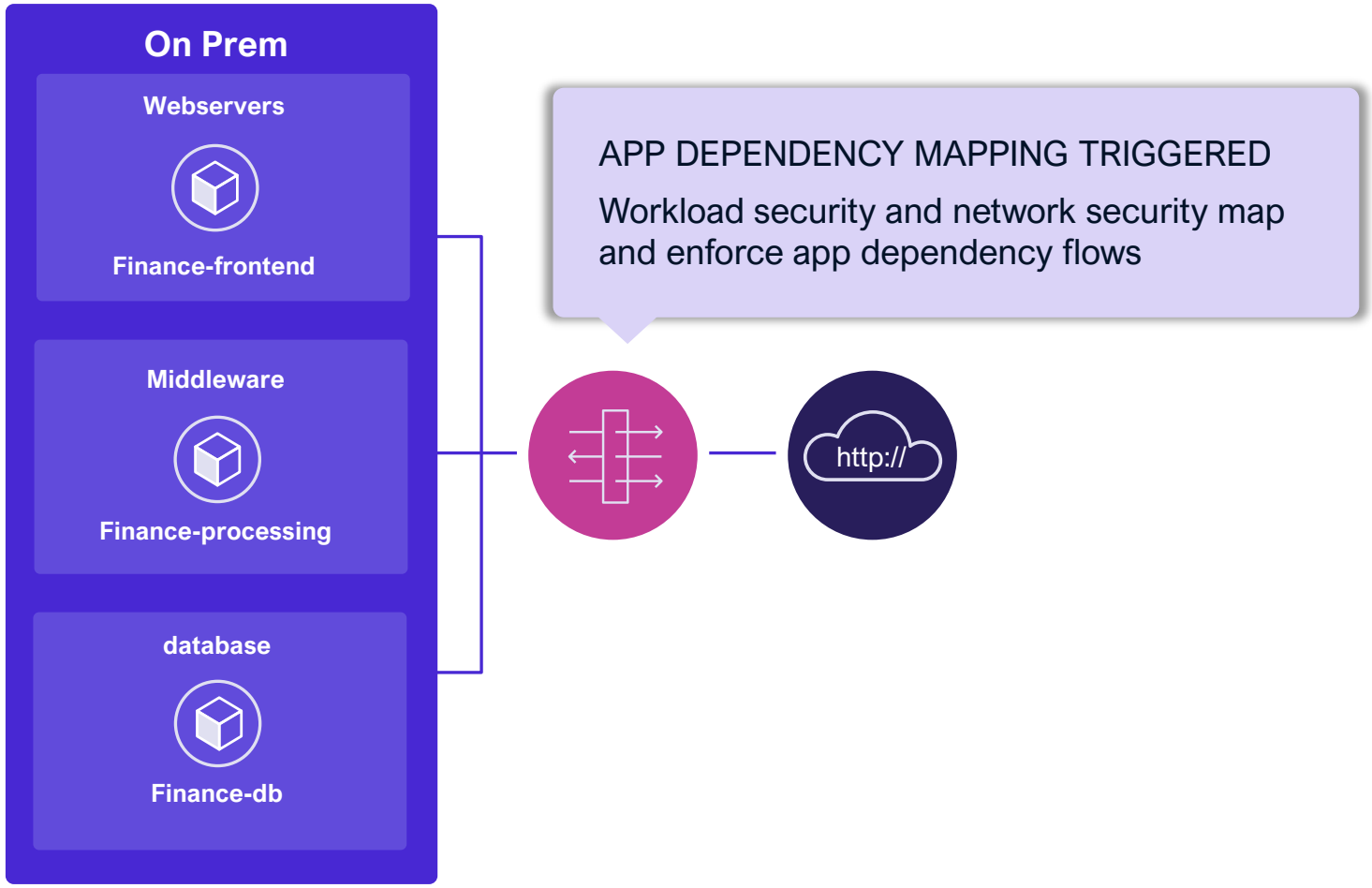
Flow-based rule

Allow	PCI_APP1	connect to	PCI_APP2	TCP/3306

Process-based rule

Allow	PCI_APP1		PCI_APP2	
	“payment_processor”	connect to	“mysqld”	TCP/3306

- Prevent malicious TLS
- **Secure application**
- Identify vulnerabilities
- Deploy / secure cloud environments
- Prevent exploits



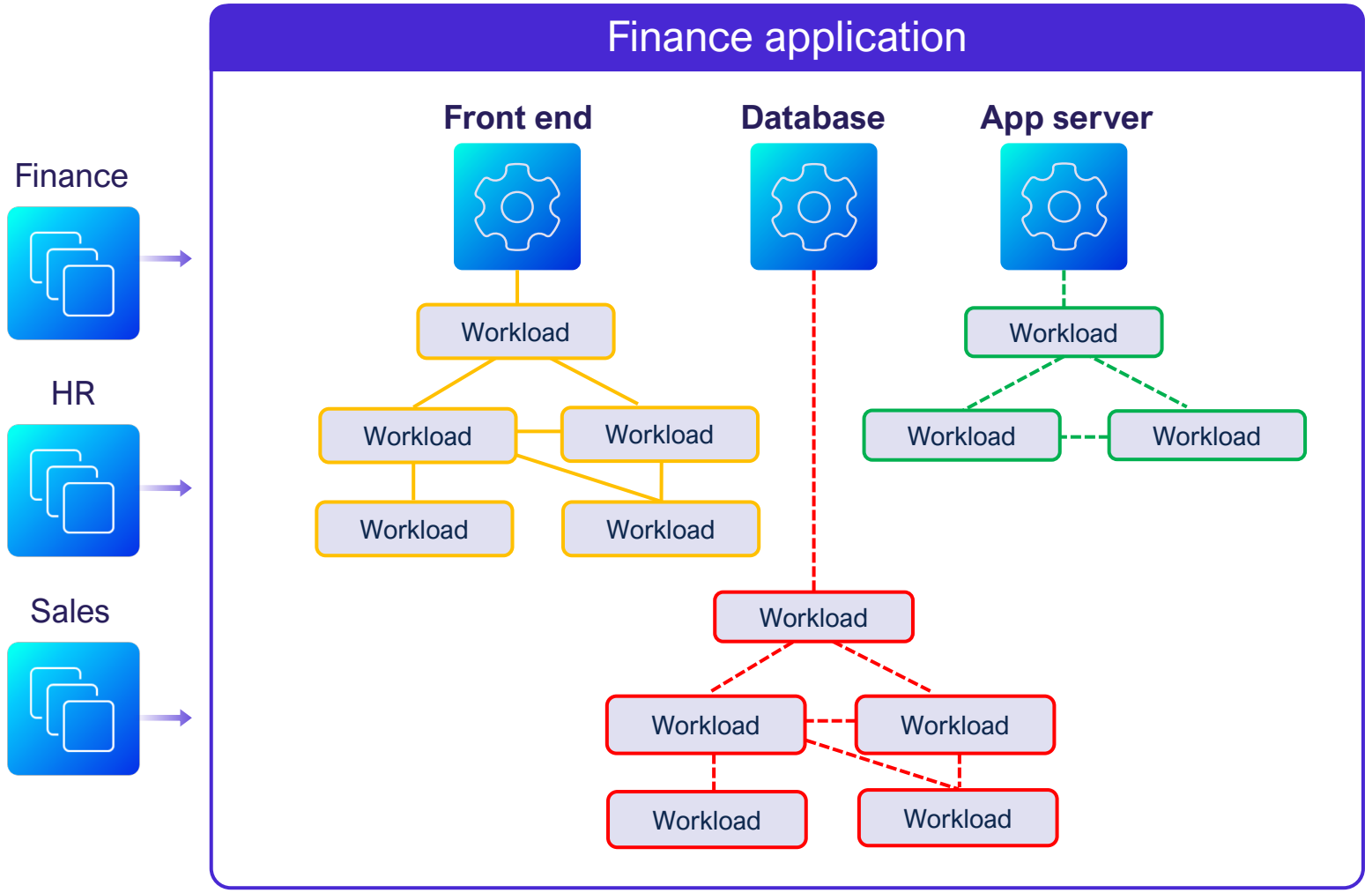
Discover and prioritize risk

Accurate
vulnerability discovery

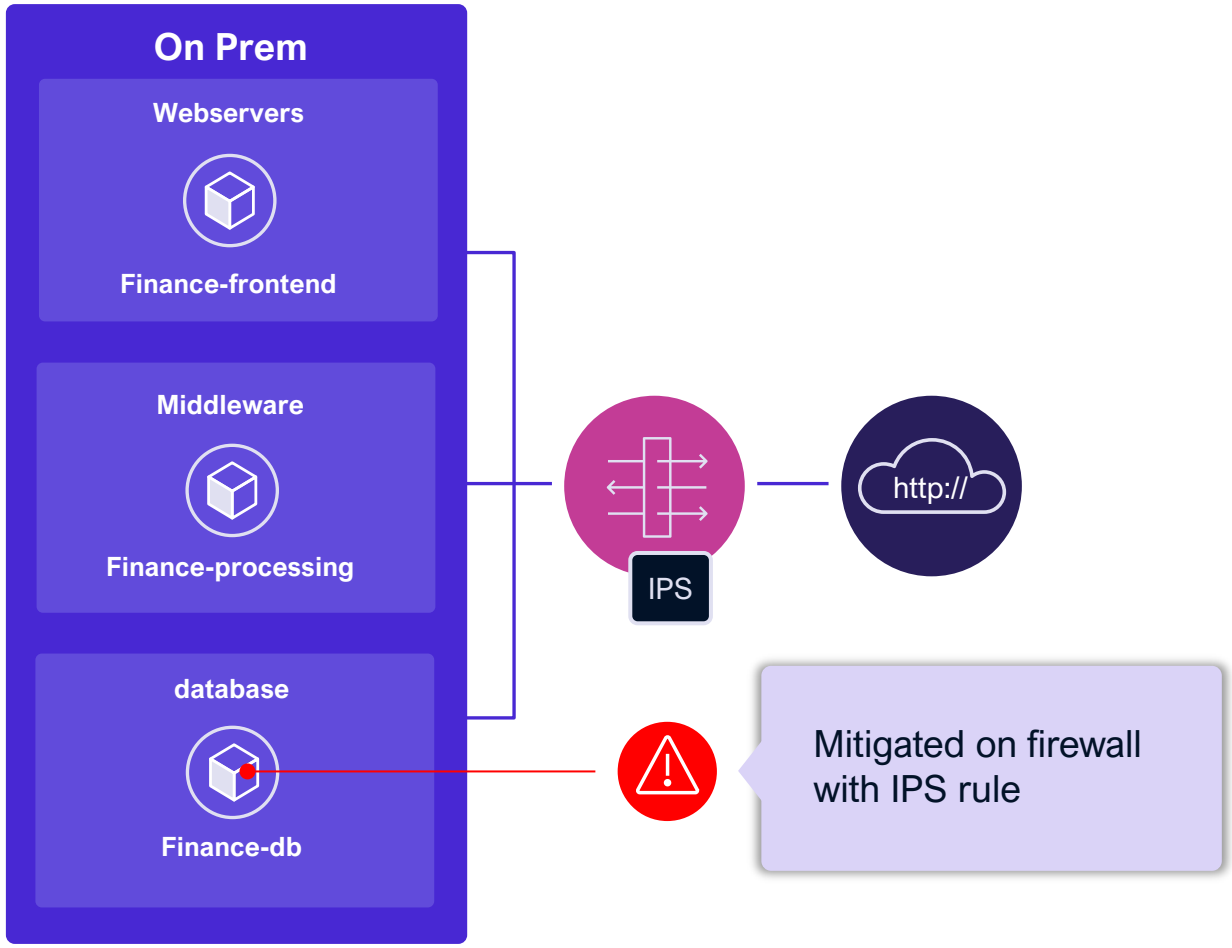
Data-driven vulnerability
prioritization

Optional augmentation
from third-party scanners

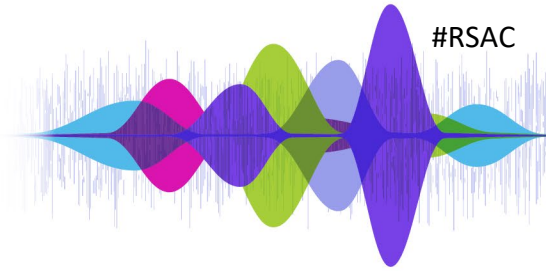
Understand zero-day variants



- Prevent malicious TLS
- Secure application
- **Identify vulnerabilities**
- Deploy / secure cloud environments
- Prevent exploits



Cloud-native Firewall

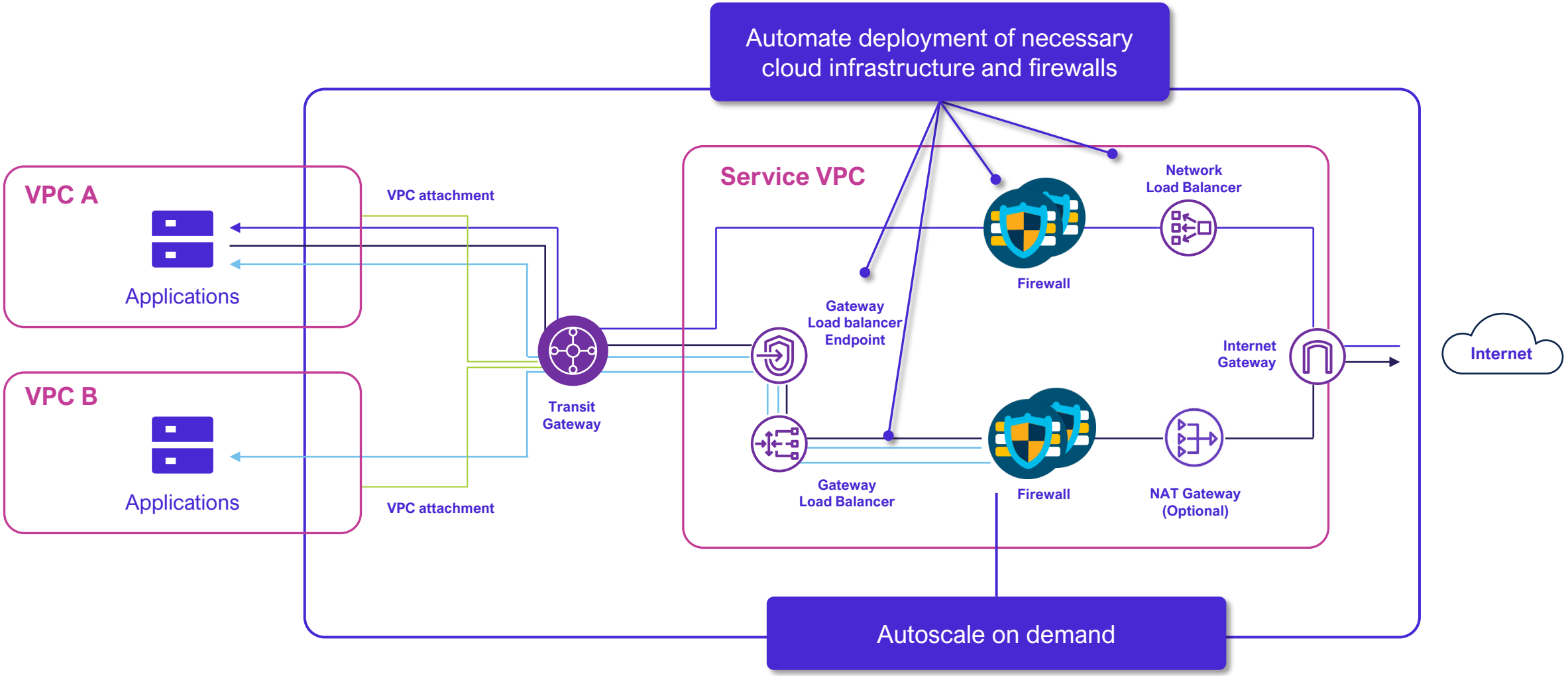


Automated Deployment

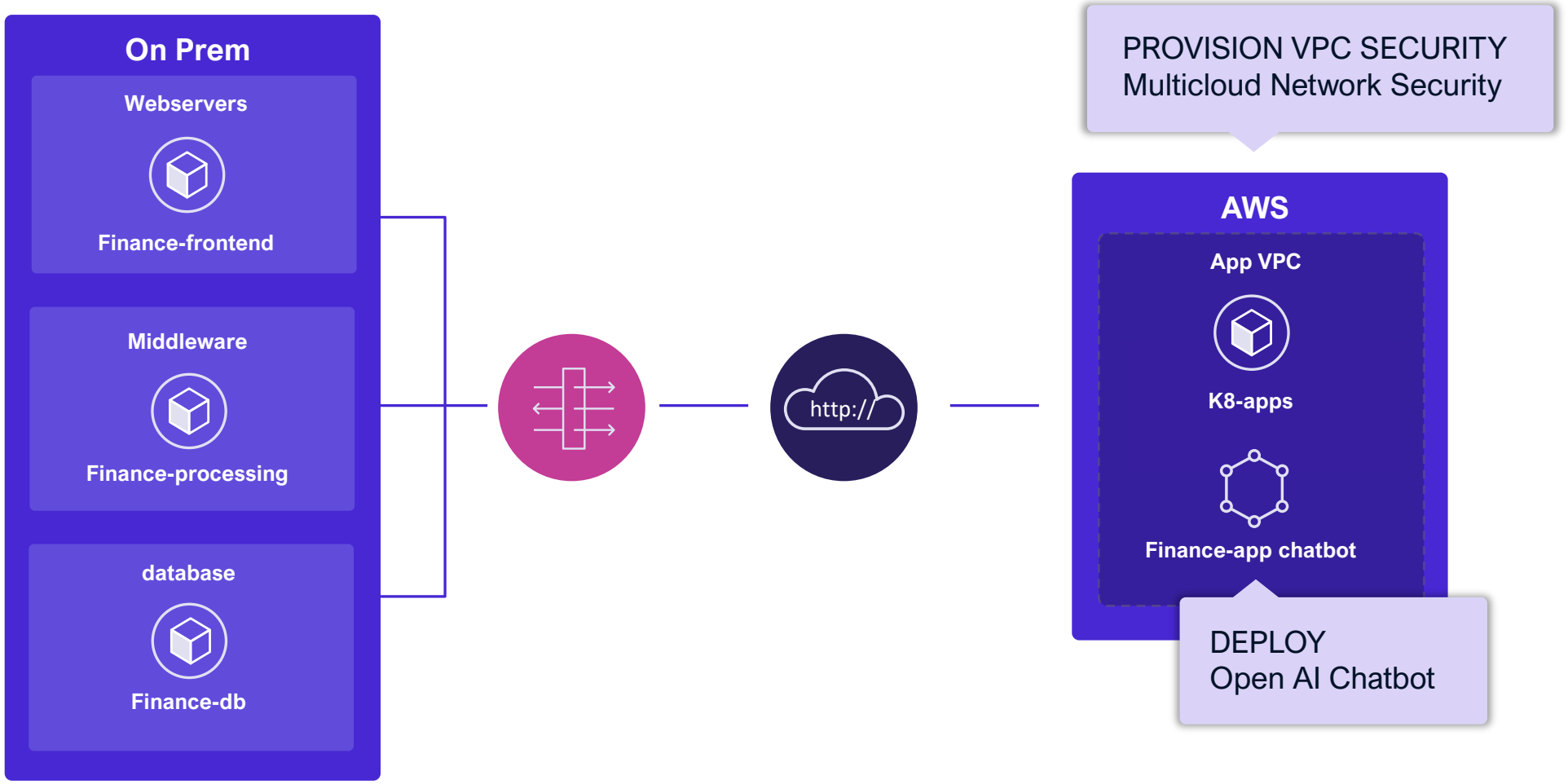
Auto-scaling

Self-healing

Enables firewalling at scale across multi-cloud environments


Automate deployment of necessary cloud infrastructure and firewalls
VPC A
Applications
VPC B
Applications
VPC attachment
VPC attachment
Transit Gateway
Service VPC
Gateway Load balancer Endpoint
Gateway Load Balancer
Firewall
Firewall
Network Load Balancer
Internet Gateway
NAT Gateway (Optional)
Internet
Autoscale on demand

- Prevent malicious TLS
- Secure application
- Identify vulnerabilities
- **Deploy / secure cloud environments**
- Prevent exploits



AI model protection

Recommended Actions

Protect applications (67)

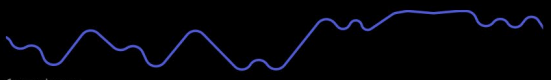
Secures sensitive data, prevents unauthorized access, and protects proprietary algorithms from theft or misuse.

Hide View →

Review increased app usage 3 days ago

Review sudden spikes in blocked events to avoid security risks.

ExternalChatBot Application
45MB +7%



1 week ago

Hide View →

Review third party apps (67) 3 days ago

Safeguards user privacy, prevents data breaches, and ensures compliance with security and regulatory standards.

Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Protection: Guardrail Categories

Security

- Prompt Injection
- Denial of service
- Cybersecurity and hacking
- Code presence
- Adversarial content
- Malicious URL

Privacy

- IP Theft
- PII
- PCI
- PHI
- Source code

Safety

- Financial harm
- User harm
- Societal harm
- Reputational harm
- Toxic content

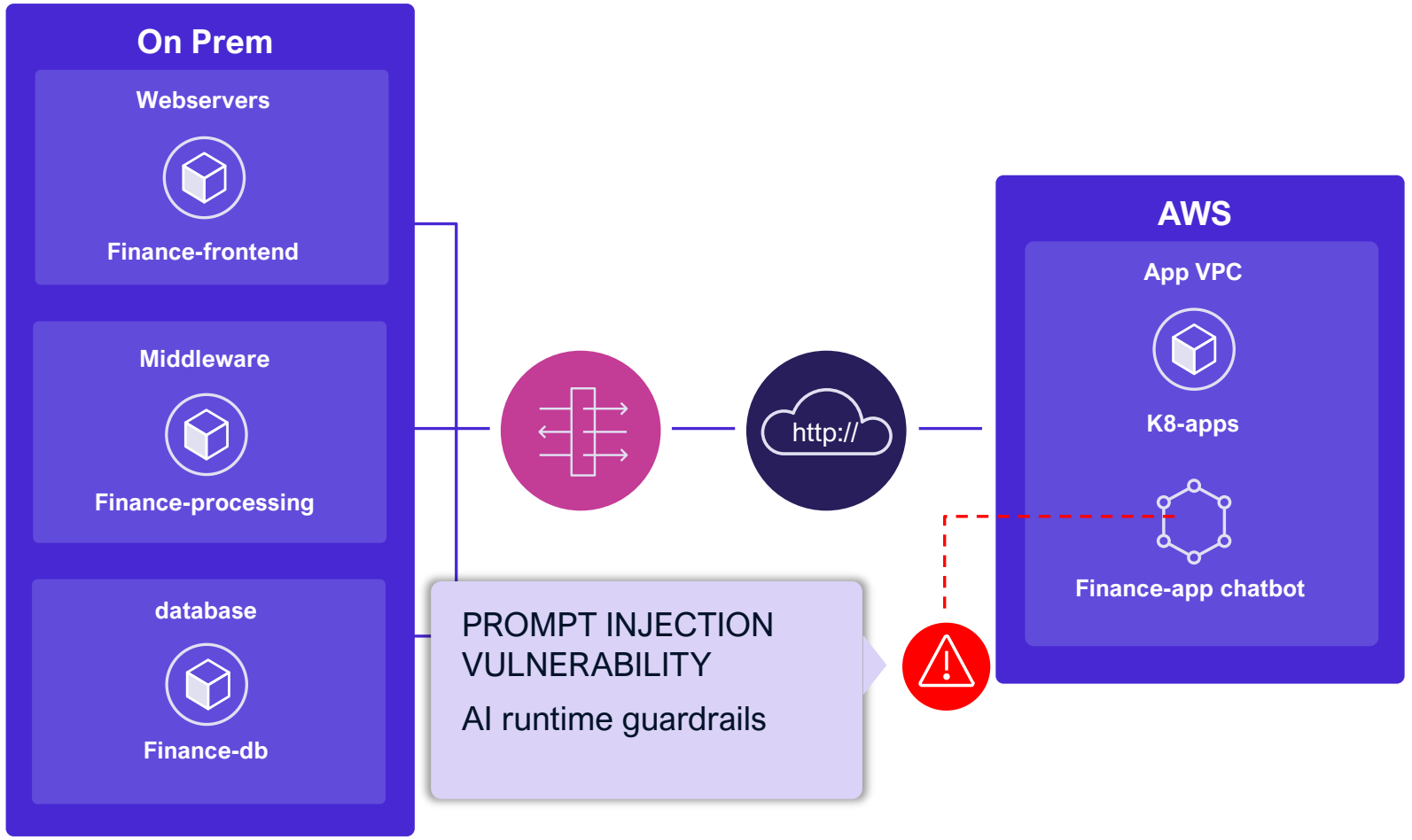
Relevancy

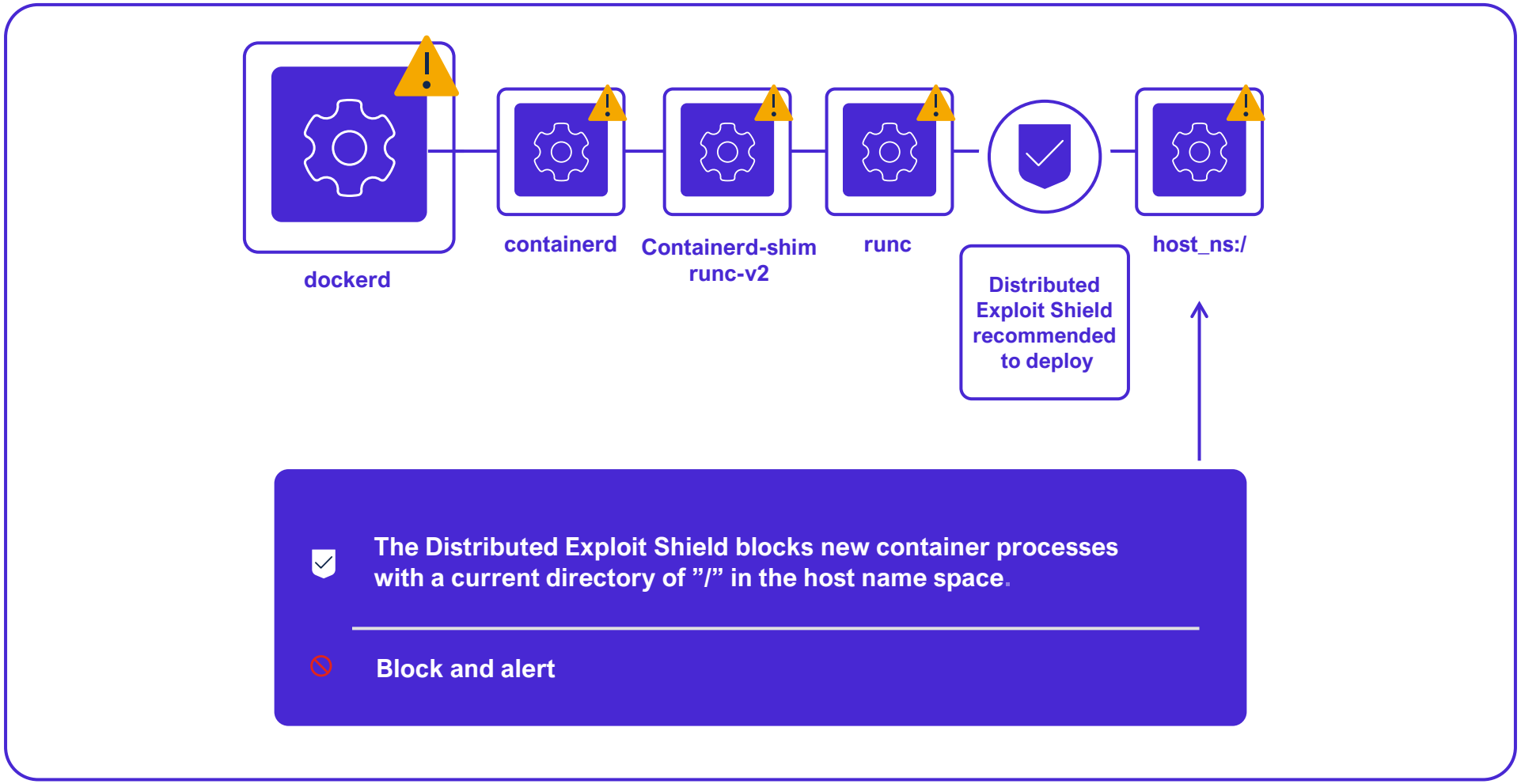
- Content moderation
- Hallucination
- Off-topic content

Map guardrails to standards and frameworks: OWASP MITRE ATLAS

Guardrails can be modified to fit industry, use case, or preferences

- Prevent malicious TLS
- Secure application
- Identify vulnerabilities
- Deploy / secure cloud environments
- **Prevent exploits**

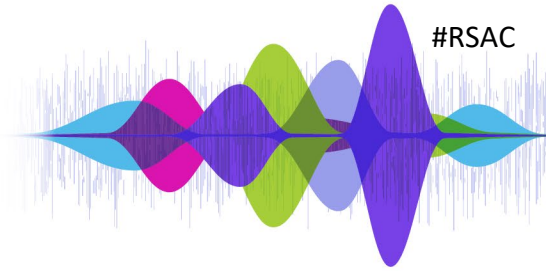




Surgical mitigating control in the path of the process that keeps application running

- Prevent malicious agent
- Secure application
- Identify vulnerabilities
- Deploy / secure cloud environments
- **Prevent exploits**

Next Steps



Apply

- Take core capabilities learned within presentation and determine how this approach can benefit your organization today
- Implement a unified segmentation strategy that aligns with your objectives (regulatory compliance, internal mandate, customer requirement)
- Skillfully deal with encrypted traffic at scale
- Assess your risk of your current AI applications and models; apply guard rails for safe and secure use of AI

Questions?

RSAC™ 2025 Conference

Thank you

Many Voices.
One Community.